

# SEQUENCING LONE-ACTOR TERRORIST BEHAVIOURS

Paul Gill

University College London

## FEIN & VOSSEKUIL (1999)

- “Attacks...result from an understandable and discernible process of thinking and behaviour”

## GILL ET AL. (2014)

- Forget socio-demographics
- Focus on behaviour
- Leakage is common
- Wide range of activities precede radicalisation
- Mental health problems and psychological distress are common
- Many engaged in activities in a wider ideological social milieu
- Rarely sudden and impulsive



## IDEOLOGICAL ATTAINMENT

- "Vulnerability" embedded within policy
- In Prevent Guidance those said to be 'vulnerable' include
  - "people with mental health issues or learning disabilities" (p.83),  
those who religiously "convert" due to them being "initially less well-informed about their faith" (p.87) and "young offenders and people vulnerable to offending" (p.91).

Corner, Bouhana & Gill, (Forthcoming)

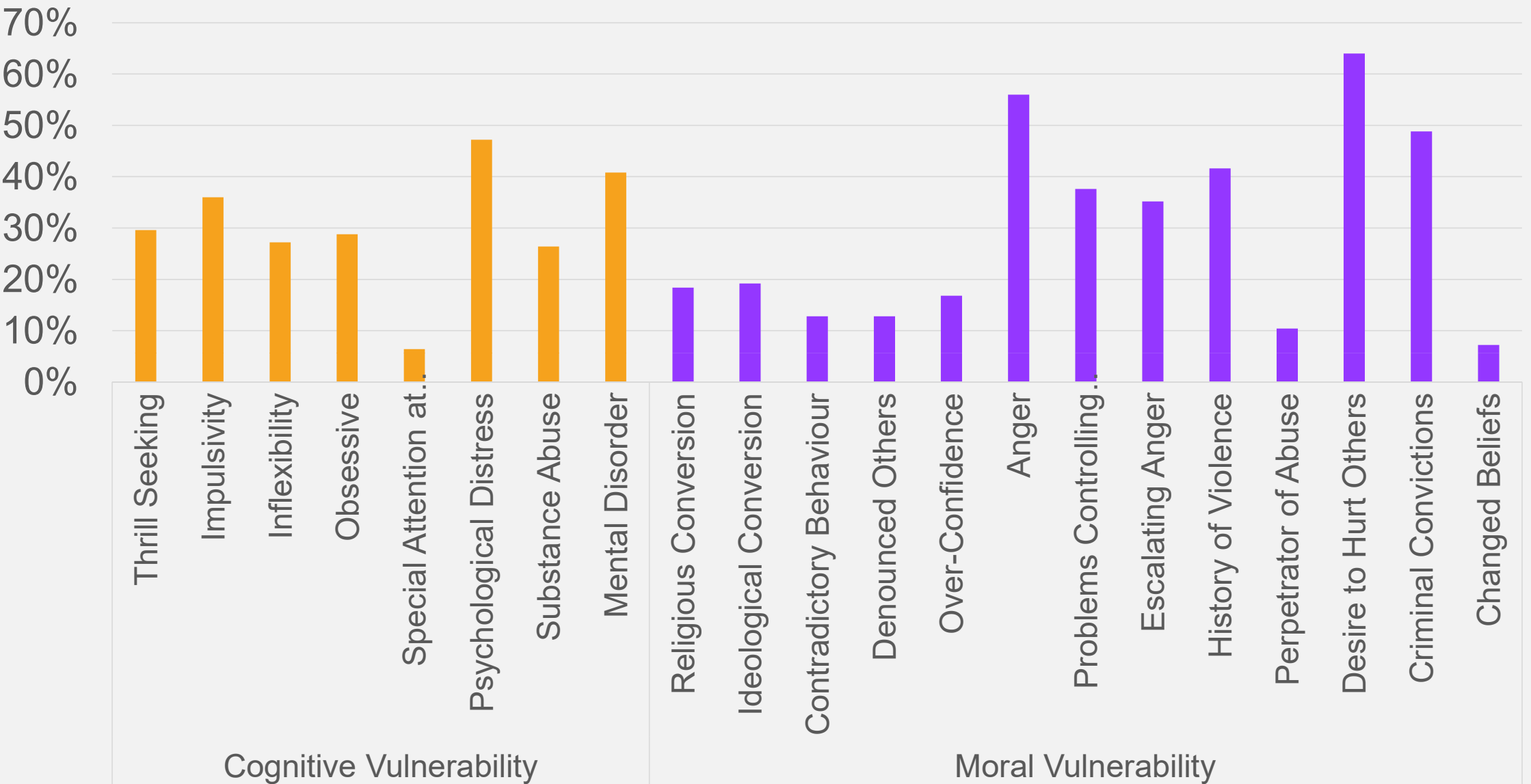
## TYPES OF VULNERABILITY

- Cognitive
  - Thrill seeking, Impulsive, Inflexible, Obsessive Tendencies
  - School difficulties, psychological distress, substance abuse, mental disorder
- Moral
  - Conversions, Behaviour contradictory to an espoused ideology, Denouncing Co-Ideologues, Anger, Abusive, History of Violence, Criminal Past

## TYPES OF SELECTION

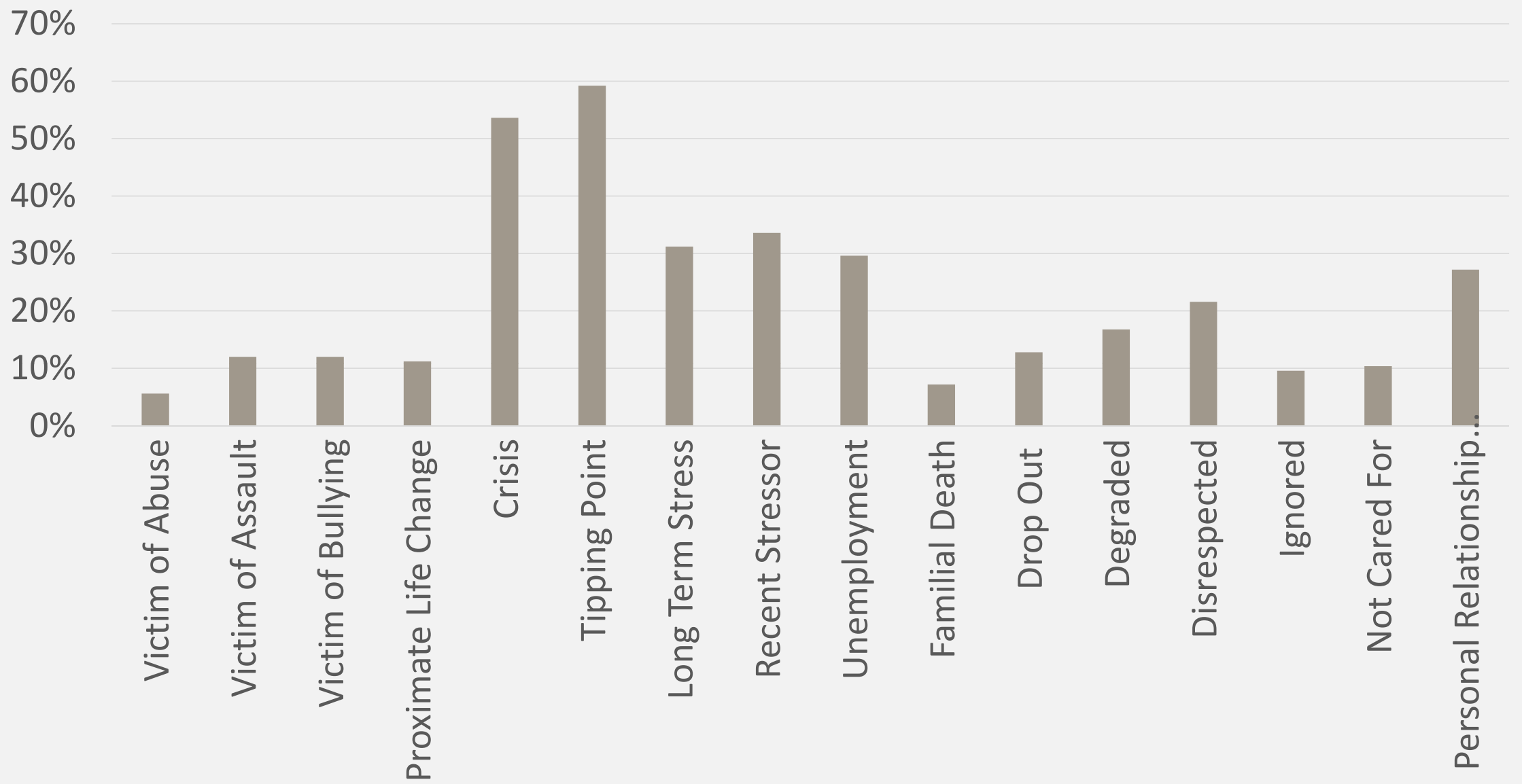
- Self Selection
  - Push Factors
- Social Selection
  - Pull Factors

# Vulnerability

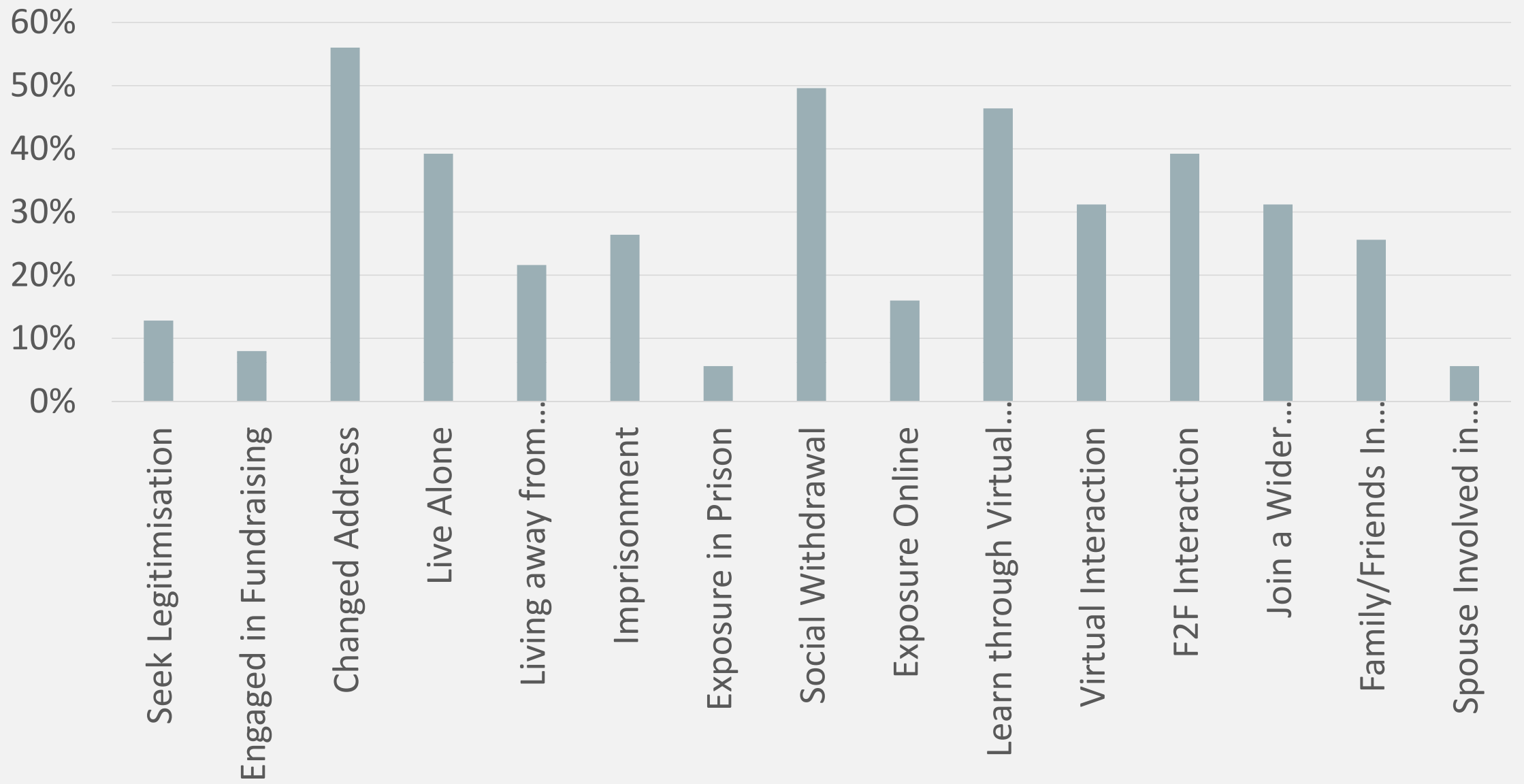


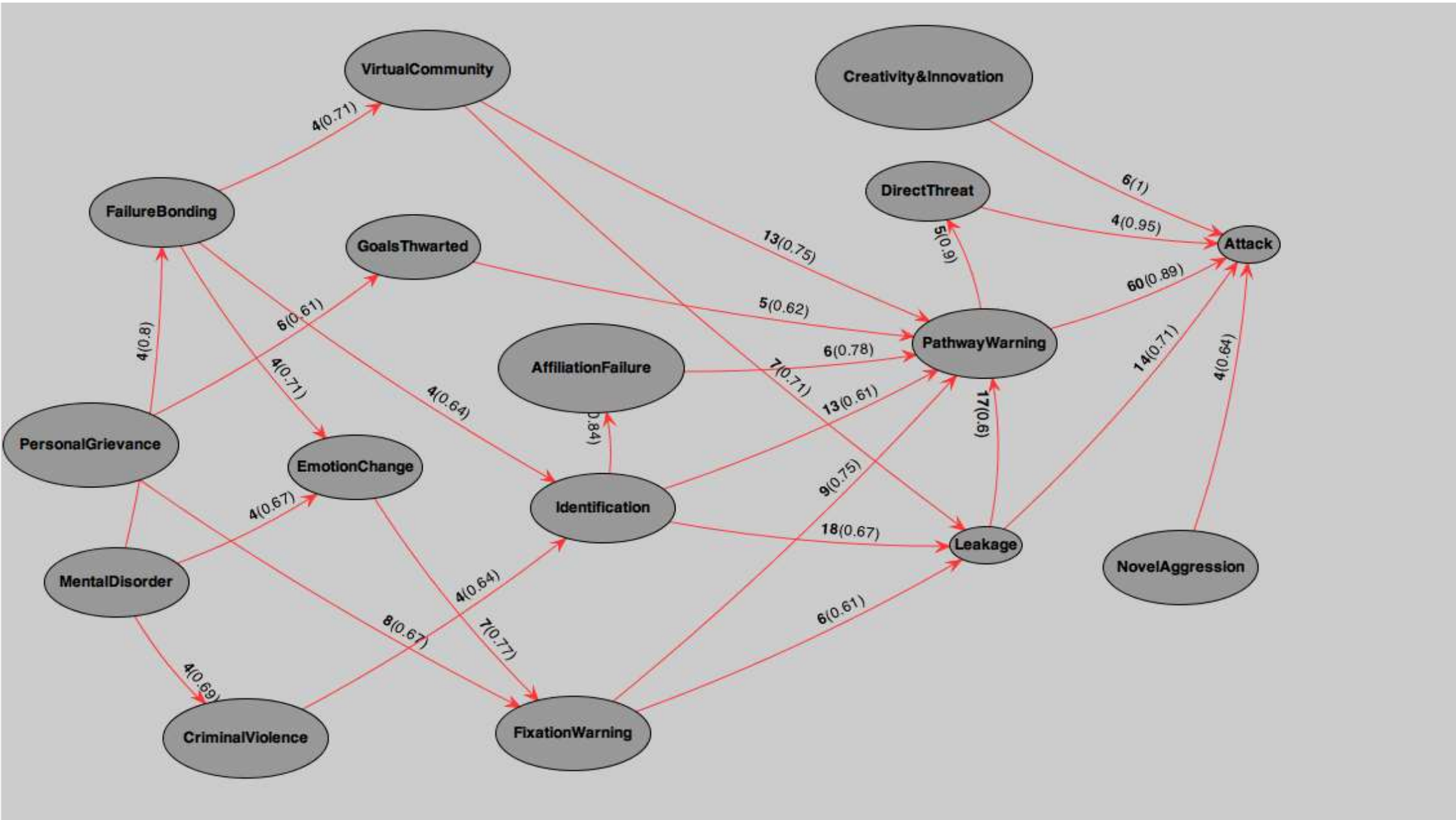


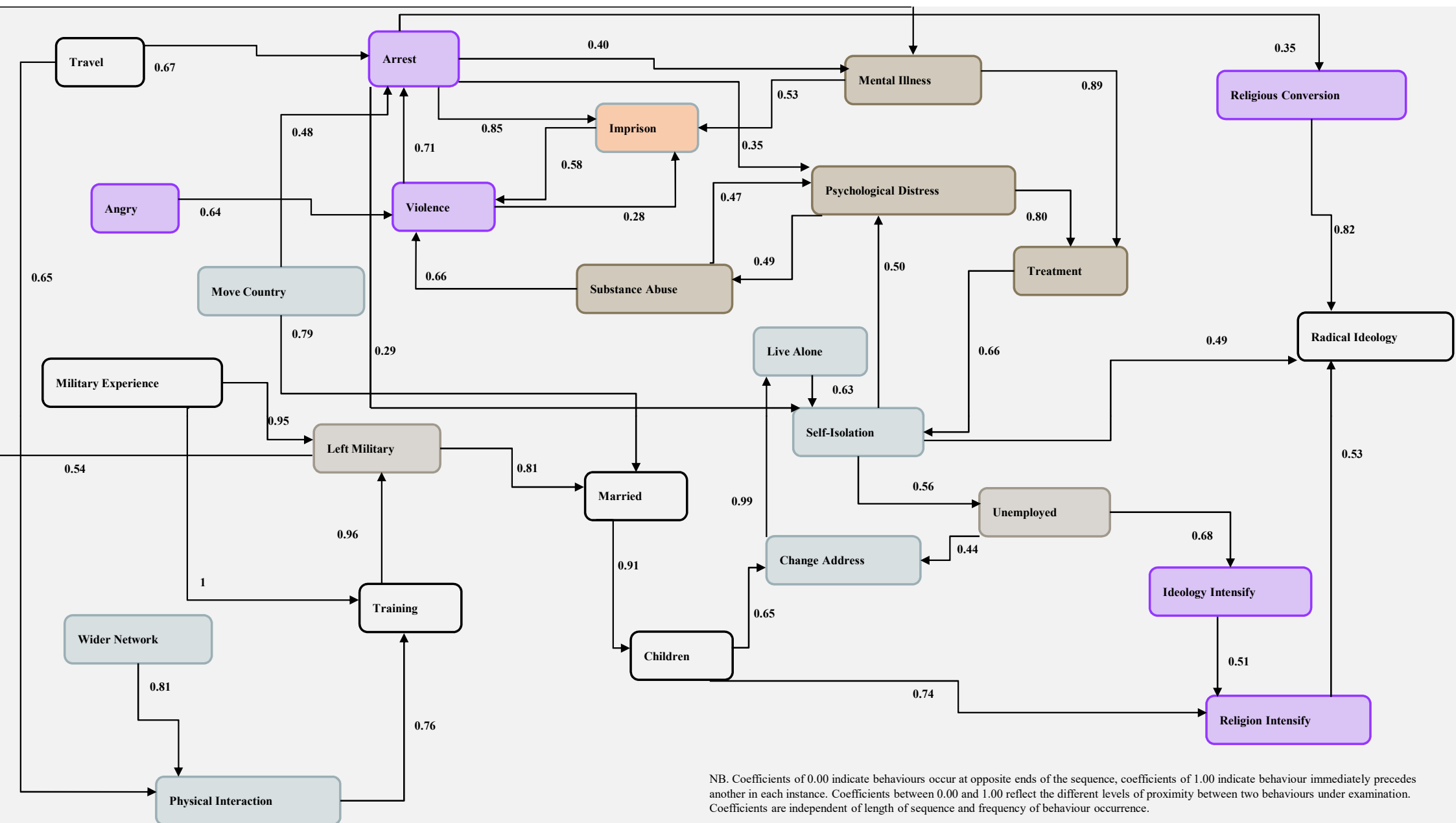
## Self-Selection



## Social Selection







NB. Coefficients of 0.00 indicate behaviours occur at opposite ends of the sequence, coefficients of 1.00 indicate behaviour immediately precedes another in each instance. Coefficients between 0.00 and 1.00 reflect the different levels of proximity between two behaviours under examination. Coefficients are independent of length of sequence and frequency of behaviour occurrence.

## THE ONLINE SPACE

- Real lack of data
- 6.5% of studies used some form of data
- Just 2% used primary data
- Lack of psychological (1%) and criminological (0%) research

## GILL ET AL. (2017)

- Looks at 227 U.K. based convicted terrorists
- Codes for online-related behaviour
- 1990-2014

## GILL ET AL. (2017)

- 61% of cases displayed evidence of online activity related to their attack/conviction
- Just over half (54%) of all actors used the Internet to learn about some aspect of their intended terrorist activity. From 2012 onwards, the figure is 76%.
- 32% prepared for their attacks using online resources
- 29% communicated with others virtually
- 15% of actors disseminated propaganda online
- 9% sought to recruit others online.
- 5% sought legitimisation for future actions from epistemic authority
- 5% also signalled online their plans to engage in attacks prior to the attack itself

## THOSE WHO ENGAGED IN ONLINE LEARNING ACTIVITIES

- Significantly more likely XRW (attack planning)
- Significantly more likely to attempt harder targets
- Less likely to have military backgrounds
- Significantly more likely to use IEDs
- Significantly less likely to use primitive attack types
- Significantly more likely to be lone actors
- More likely to have offline interactions also



## THOSE WHO COMMUNICATED ONLINE

- Significantly more likely amongst the extreme-right wing cohort
- Significantly less likely to target military
- Significantly more likely to use IEDs
- Significantly more likely to be accompanied with face-to-face interactions with non-violent co-ideologues

## LEAKAGE

- 86.5% - others were aware of the individual's personal grievances, extreme ideology, and their desire to hurt others
- Over 50% - , others were aware that the individual in question had attack equipment
- When leakage occurs, 58% regarding weapon and 66% regarding target
- "Leakers" significantly more likely to have a violent past. Around a third of recipients aware of individual's prior violence.
- 32% occurs within a week of the attack

Consequences	Average	Right Wing	Jihadist	Single issue
No further action	37.8%	33.3%	39.3%	42.1%
Provided aid	9.5%	11.1%	14.3%	0
Police knew and did not prevent it	4.1%	7.4%	0	15.8%
Police knew and no further action	9.5%	7.4%	10.7%	10.5%
Reported, arrested and thwarted	17.6%	22.2%	14.3%	10.5%
Too late	5.4%	11.1%	0	5.3%
Caught post attack	6.8%	11.1%	3.6%	5.3%
Leakage not seen	6.4%	0	7.1%	15.8%

Purpose:	Average	Right Wing	Jihadist	Single issue
Unburden	33.8%	26%	46.4%	26.3%
Threats	43.2%	59.3%	25%	47.4%
Help	32.4%	22.2%	39.3%	36.8%
Mentally ill	12.2%	14.8%	3.6%	15.8%
Prevention	1.4%	0	0	5.3%
Use of facilities	6.8%	3.7%	10.7%	5.3%
Suicide note	1.4%	3.7%	0	0

Instances	Average	Right Wing	Jihadist	Single issue
Once	40.5%	48.1%	28.6%	42.1%
Multiple (3-5)	29.7%	22.2%	38.3%	26.3%
Extensive (5+)	29.7%	33.3%	25%	31.6%

Form:	Average	Right Wing	Jihadist	Single issue
Social media	17.6%	14.8%	25%	10.5%
Website	6.8%	4.2%	3.5%	15.8%
Email	12.2%	14.8%	14.2%	5.2%
Verbally	68.9%	63%	64.3%	78.9%
Letters	13.5%	18.5%	7.1%	15.7%
Other	2.7%	3.7%	3.6%	0

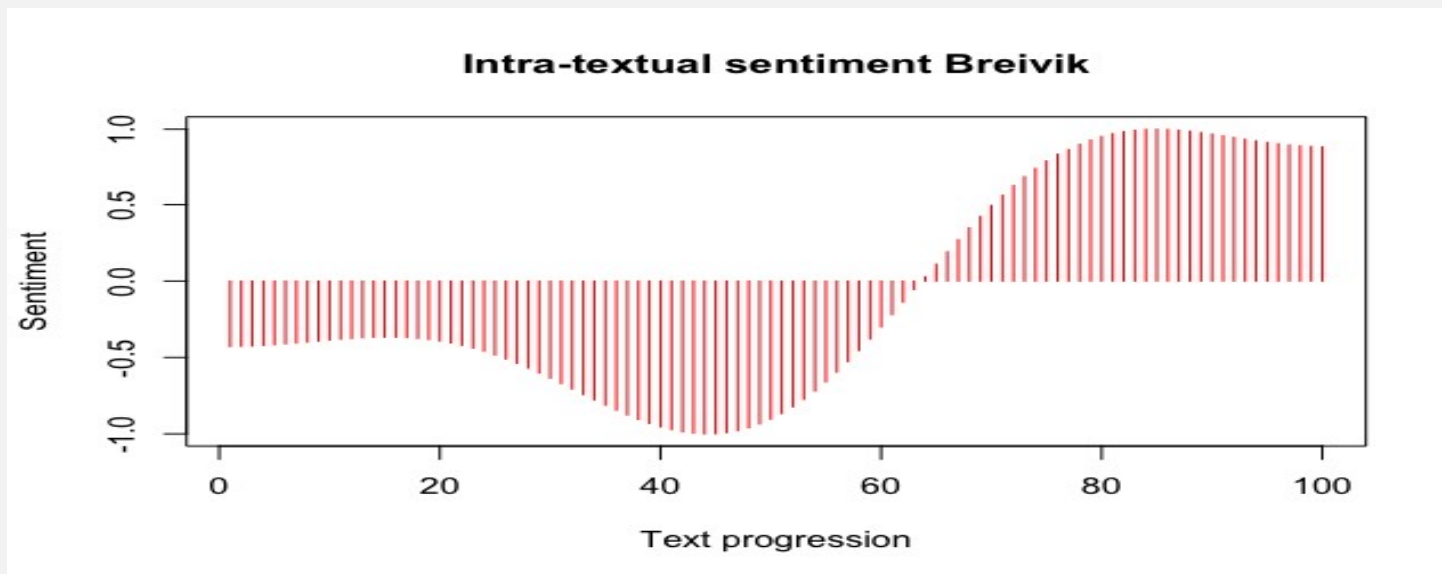
Recipients	Average	Right Wing	Jihadist	Single issue
Friends	36.5%	35.7%	42.3%	31.6%
Family	14.9%	7.1%	19.2%	21.1%
Accomplices	23%	25%	23.1%	21.1%
Colleagues	8.1%	7.1%	7.7%	10.5%
Target	6.8%	10.7%	0	10.5%
Mental health staff	6.8%	3.6%	3.8%	10.5%
Partner	9.5%	14.3%	3.8%	10.5%
Stranger	23%	28.6%	15.4%	26.3%
Law Enforcement	20.3%	11.1%	25%	26.3%

# BROADCASTING IDEOLOGY



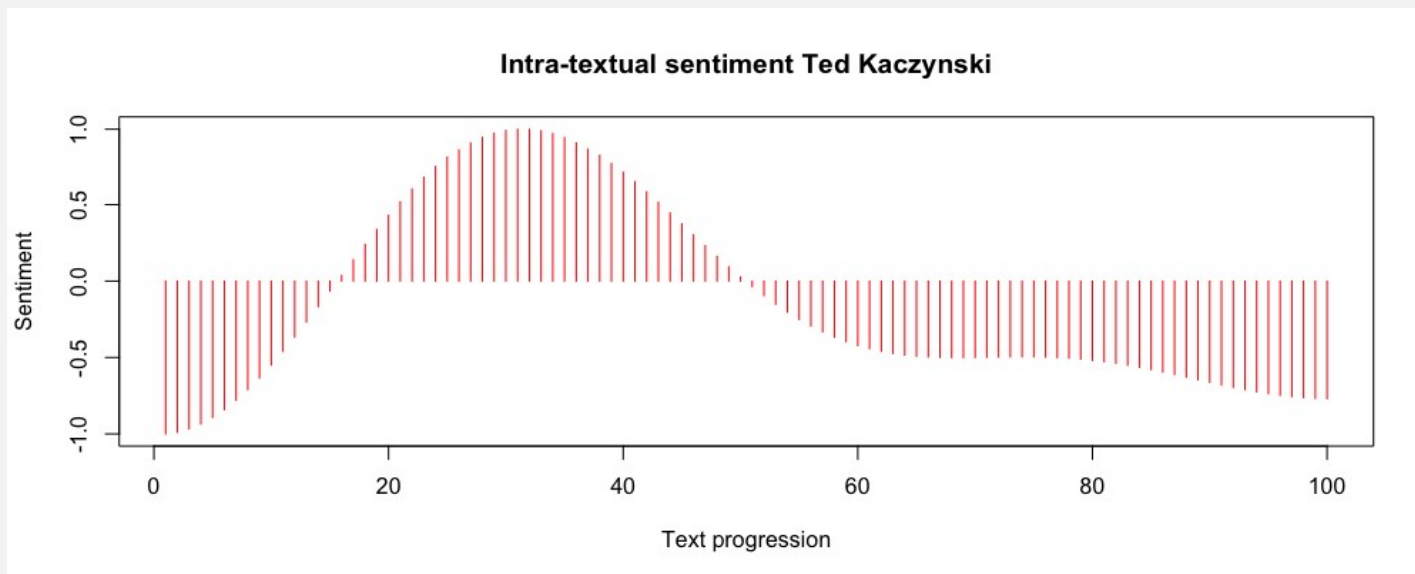


# ANDERS BREIVIK



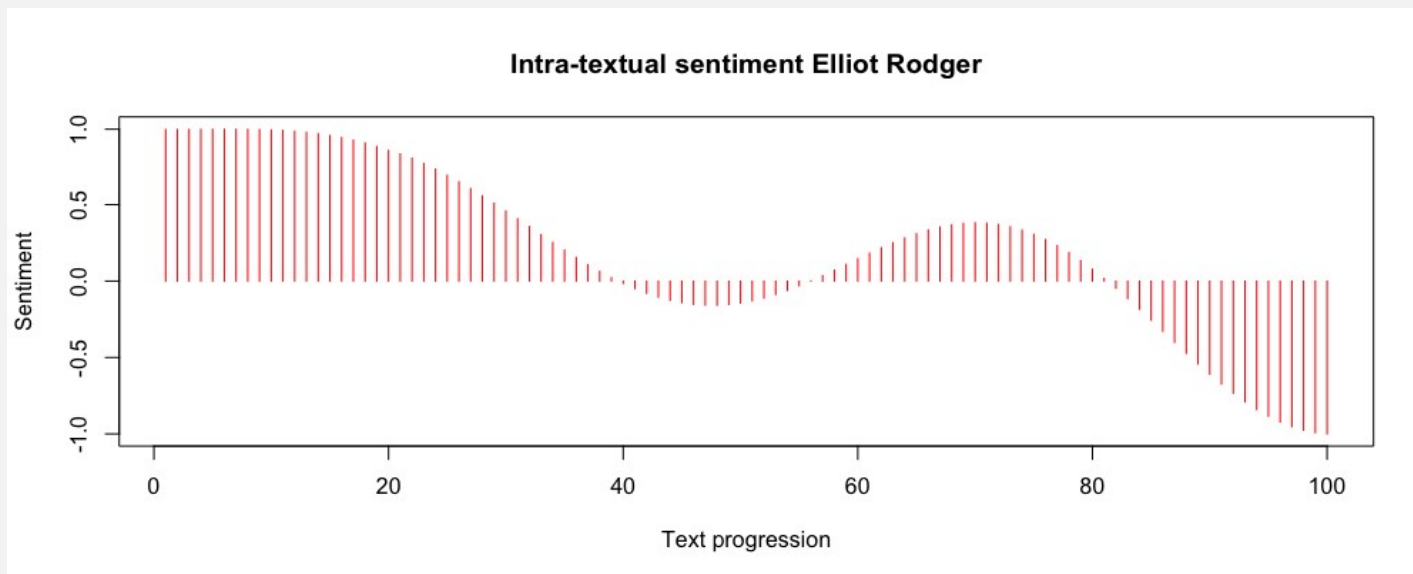
Van Der Vegt, Kleinberg & Gill (In Progress)

# TED KACZYNSKI



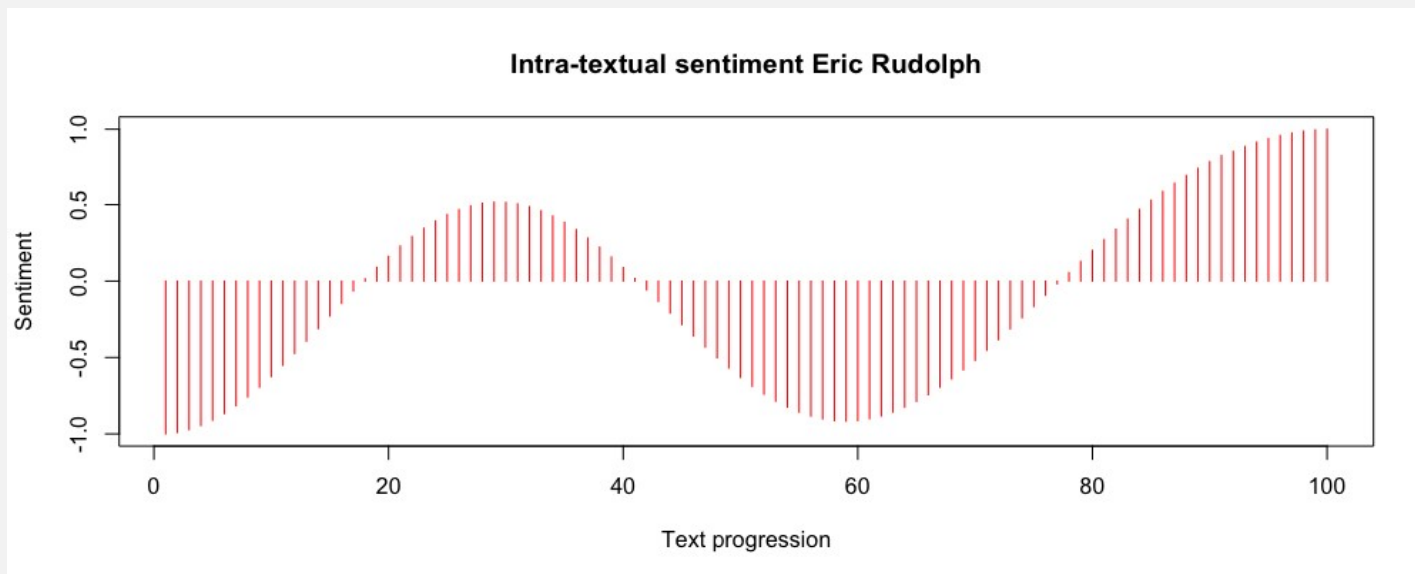
Van Der Vegt, Kleinberg & Gill (In Progress)

# ELLIOT RODGER



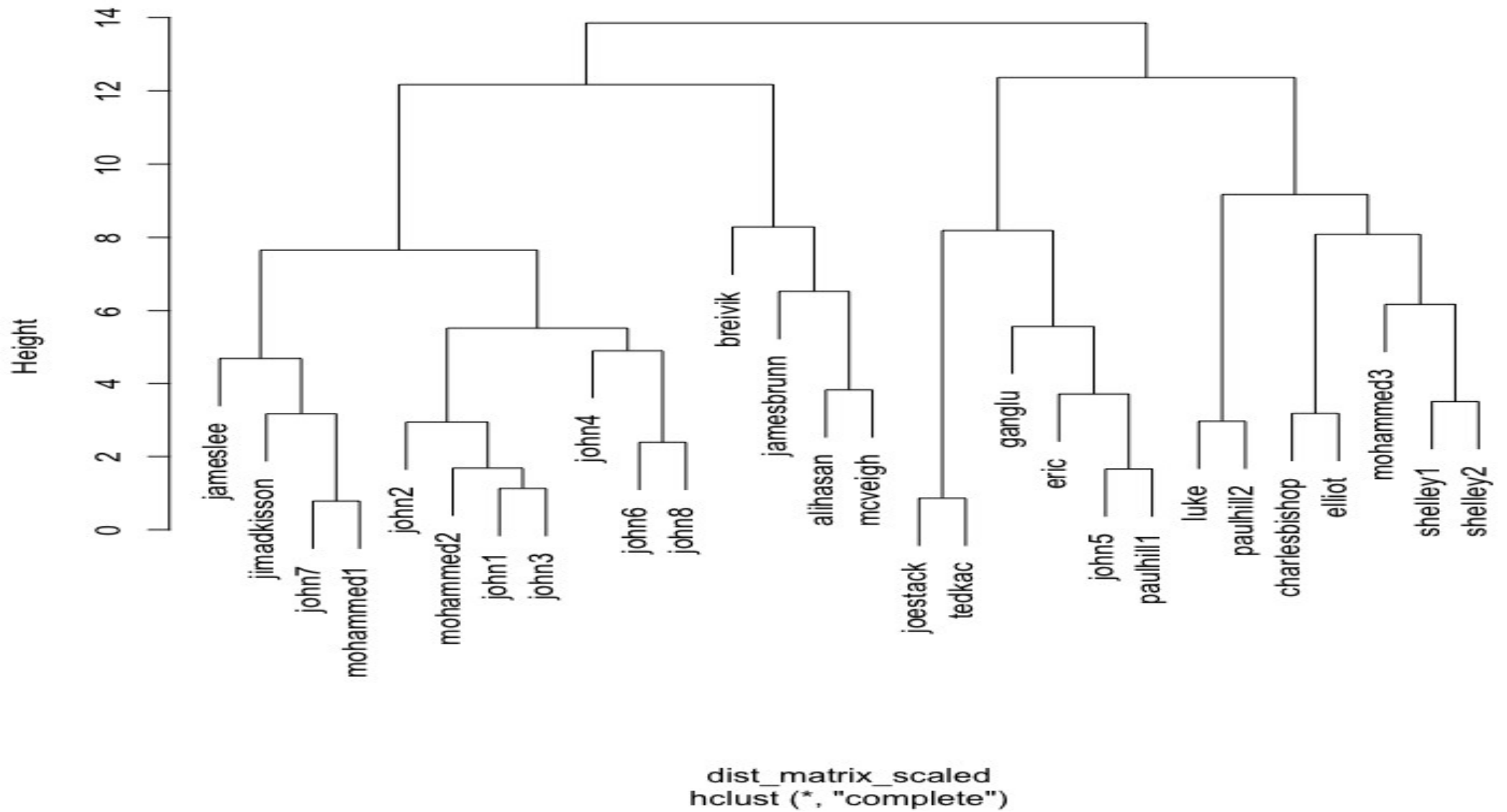
Van Der Vegt, Kleinberg & Gill (In Progress)

# ERIC RUDOLPH



Van Der Vegt, Kleinberg & Gill (In Progress)

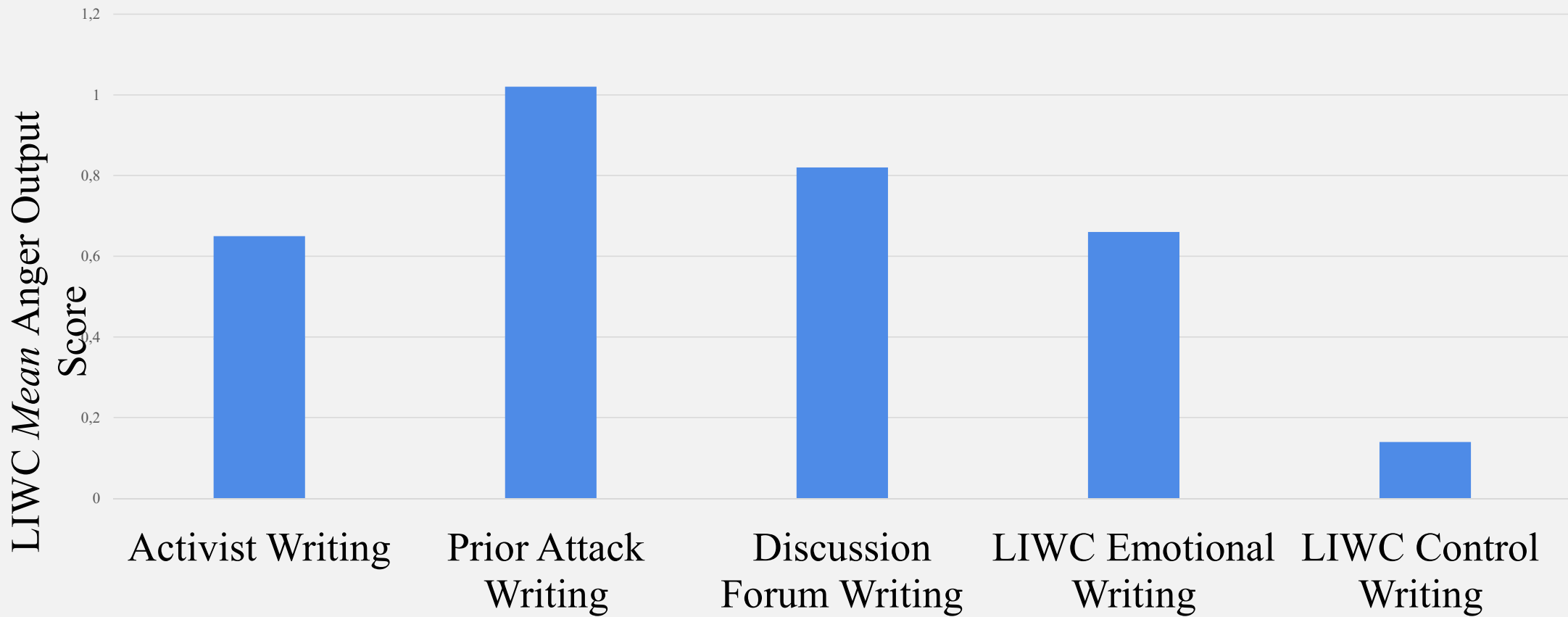
Cluster Dendrogram



## LINGUISTIC ANALYSIS, SENTIMENT AND COGNITION

- 20 lone actor and mass murder manifestos
- 500 randomly selected 'long' forum posts on StormFront
- 19 non-violent activist writings
- *Linguistic Inquiry and Word Count (LIWC) software*

## LIWC *Mean* Anger Score



Doherty and Gill (In Preparation)

## DISCERNING SIGNAL FROM THE NOISE

- 2118 Threats made to U.K. Public Figures
  - Royal Family & Members of Parliament
  - Threats communicated both online and offline
  - Background “offender” information
  - Follow-up information
    - Those who did nothing
    - Those who showed up and did nothing
    - Those who showed up and tried something



## APPROACHERS VS. COMMUNICATORS

- Those Who Approached
  - Significantly More Likely
    - Police Record
    - Substance Problem
    - Violence
    - Evidence of Overt Mental Disorder
    - Grandiose Language
    - 'Deluded' Content
  - Significantly Less Likely
    - History of Harassment
    - 'Rambling' Content
    - Help Seeking

## THEORY: ARE ONLINE THREATS MORE RISKY?

No

- Just 'Keyboard Warriors'

- Less effort

- Less time consuming

- less risk of detection possibly

- Easier access to communicate to principal target

- Wider milieu leading to anonymization/groupthink/all social psych explanation

- Online threats more likely to
  - involve a subsequent approach\* (almost twice as likely)
    - BUT less likely to attempt a 'breach (13 times less likely)''\*\*\*
- Maybe a result of different targets of fixation or individual characteristics
  - Online threats more likely against politicians, Sites, embassies\*\*\*
- Online threateners more likely to Have
  - police criminal record\*\*\*
  - Harassment history\*\*\*
  - Threats History\*\*
  - Firearms access\*\*
- Online threateners more likely depicted as
  - Persecuted, Homicidal ideation, resentful persecuted, resentful agenda
- Online threats more likely coded as
  - Demanding, abusive, angry

Key: \*=<.05; \*\*=<.01; \*\*\*=<.001

## TERRORIST DECISION-MAKING: A PRIMER

- It looks like criminal decision-making
- Subjective 'feelings' play a large role
- Terrorists often keep several potential targets in mind and choose the one with the relatively fewest risks.
- The cost–benefit analyses differ across terrorist groups and terrorists because risk preferences differ.
- Prior successful experiences decrease averseness to risk
- The weighing of security features necessitates hostile reconnaissance which itself offers risk to the terrorist in terms of detection.
- What matters are perceptions of how effectively deployed security is

Gill et al. (2018) • Third-parties often play key roles in gaining intelligence for an attack

THANK YOU

- Contact - [Paul.Gill@ucl.ac.uk](mailto:Paul.Gill@ucl.ac.uk)
- Twitter - paulgill\_ucl
- Web – [www.grievance-erc.com](http://www.grievance-erc.com)